Electronic Version
Stylesheet Version v1.1.1

Claims

[c1] A smartcard transaction system configured with a biometric security system, said system comprising:
a smartcard configured to communicate with a reader;
a reader configured to communicate with said system;
an auditory emissions scan sensor configured to detect a proffered auditory emissions scan sample, said auditory emissions scan sensor configured to communicate with said system; and,
a device configured to verify said proffered auditory emissions scan sample to facilitate a transaction.

[c2] The smartcard transaction system of claim 1, wherein said sensor is configured to communicate with said system via at least one of a smartcard, a reader, and a network.

[c3] The smartcard transaction system of claim 1, wherein said auditory emissions scan sensor is configured to facilitate a finite number of scans.

[c4] The smartcard transaction system of claim 1, wherein said auditory emissions scan sensor is configured to log at least one of a detected auditory emissions scan sam-

ple, processed auditory emissions scan sample and stored auditory emissions scan sample.

[c5] The smartcard transaction system of claim 1, further including a database configured to store at least one data packet, wherein said data packet includes at least one of proffered and registered auditory emissions scan samples, proffered and registered user information, terrorist information, and criminal information.

[c6] The smartcard transaction system of claim 5, wherein said database is contained in at least one of the smartcard, smartcard reader, sensor, remote server, merchant server and smartcard system.

[c7] The smartcard transaction system of claim 6, wherein said remote database is configured to be operated by an authorized sample receiver.

[c8] The smartcard transaction system of claim 1, wherein said auditory emissions scan sensor device is configured with at least one of an infrared optical sensor, an auditory sensor, and a sound generator.

[c9] The smartcard transaction system of claim 1, wherein said auditory emissions scan sensor is configured to detect and verify auditory emissions scan characteristics including at least one of frequency, wavelength, and vi-

brations.

[c10] The smartcard transaction system of claim 1, wherein said auditory emissions scan sensor device is configured to detect false noise associated with a device producing electronic auditory emissions.

[c11] The smartcard transaction system of claim 1, further including a device configured to compare a proffered auditory emissions scan sample with a stored auditory emissions scan sample.

[c12] The smartcard transaction system of claim 11, wherein said device configured to compare an auditory emissions scan sample is at least one of a third-party security vendor device and local CPU.

[c13] The smartcard transaction system of claim 11, wherein a stored auditory emissions scan sample comprises a registered auditory emissions scan sample.

[c14] The smartcard transaction system of claim 13, wherein said registered auditory emissions scan sample is associated with at least one of: personal information, credit card information, debit card information, savings account information, membership information, PayPal account information, Western Union Account information, electronic bill payment information, automatic bill pay-

ment information and loyalty point information.

[c15] The smartcard transaction system of claim 14, wherein different registered auditory emissions scan samples are associated with a different one of: personal information, credit card information, debit card information, savings account information, membership information, PayPal account information, Western Union Account information, electronic bill payment information, automatic bill payment information and loyalty point information.

[c16] The smartcard transaction system of claim 14, wherein an auditory emissions scan sample is primarily associated with first user information, wherein said first information comprises at least one of personal information, credit card information, debit card information, savings account information, membership information, PayPal account information, Western Union Account information, electronic bill payment information, automatic bill payment information and loyalty point information, and wherein an auditory emissions scan sample is secondarily associated with second user information, wherein said second information comprises at least one of personal information, credit card information, debit card information, savings account information, membership information, PayPal account information, Western Union Account information, electronic bill payment information, auto-

matic bill payment information and loyalty point information, and wherein said second user information is different than said first user information.

[c17] The smartcard transaction system of claim 1, wherein said smartcard transaction system is configured to begin authentication upon verification of said proffered auditory emissions scan sample.

[c18] The smartcard transaction system of claim 1, wherein said smartcard is configured to deactivate upon rejection of said proffered auditory emissions scan sample.

[c19] The smartcard transaction system of claim 1, wherein said sensor is configured to provide a notification upon detection of a sample.

[c20] The smartcard transaction system of claim 1, wherein said device configured to verify is configured to facilitate at least one of access, activation of a device, a financial transaction, and a non-financial transaction.

[c21] The smartcard transaction system of claim 1, wherein said device configured to verify is configured to facilitate the use of at least one secondary security procedure.

[c22] A method for facilitating biometric security in a smartcard transaction system comprising: proffering an audi-

tory emissions scan to an auditory emissions scan sensor communicating with said system to initiate verification of an auditory emissions scan sample for facilitating authorization of a transaction.

[c23] The method for of claim 22, further comprising registering at least one auditory emissions scan sample with an authorized sample receiver.

[c24] The method of claim 23, wherein said step of registering further includes at least one of: contacting said authorized sample receiver, proffering an auditory emissions scan to said authorized sample receiver, processing said auditory emissions scan to obtain an auditory emissions scan sample, associating said auditory emissions scan sample with user information, verifying said auditory emissions scan sample, and storing said auditory emissions scan sample upon verification

[c25] The method of claim 22, wherein said step of proffering includes proffering an auditory emissions scan to at least one of an infrared optical sensor, an auditory sensor, and a sound generator.

[c26] The method of claim 22, wherein said step of proffering further includes proffering an auditory emissions scan to an auditory emissions scan sensor communicating with

said system to initiate at least one of: storing, comparing, and verifying said auditory emissions scan sample.

[c27] The method of claim 22, wherein said step of proffering an auditory emissions scan to an auditory emissions scan sensor communicating with said system to initiate verification further includes processing database information, wherein said database information is contained in at least one of a smartcard, smartcard reader, sensor, remote server, merchant server and smartcard system.

[c28] The method of claim 22, wherein said step of proffering an auditory emissions scan to an auditory emissions scan sensor communicating with said system to initiate verification further includes comparing a proffered auditory emissions scan sample with a stored auditory emissions scan sample.

[c29] The method of claim 28, wherein said step of comparing includes comparing a proffered auditory emissions scan sample to a stored auditory emissions scan sample by using at least one of a third-party security vendor device and local CPU.

[c30] The method of claim 28, wherein said step of comparing includes comparing auditory emissions scan characteristics including at least one of frequency, wavelength, and

vibrations.

[c31] The method of claim 22, wherein said step of proffering an auditory emissions scan to an auditory emissions scan sensor communicating with said system further comprises using said auditory emissions scan sensor to detect at least one of false noise associated with a device producing electronic auditory emissions.

[c32] The method of claim 22, wherein said step of proffering an auditory emissions scan to an auditory emissions scan sensor communicating with said system to initiate verification further includes at least one of detecting, processing and storing at least one second proffered auditory emissions scan sample.

[c33] The method of claim 22, wherein said step of proffering an auditory emissions scan to an auditory emissions scan sensor communicating with said system to initiate verification further includes the use of at least one secondary security procedure.

[c34] A method for facilitating biometric security in a smart-card transaction system comprising:
detecting a proffered auditory emissions scan at a sensor communicating with said system to obtain a proffered auditory emissions scan sample;

verifying the proffered auditory emissions scan sample; and

authorizing a transaction to proceed upon verification of the proffered auditory emissions scan sample.

[c35] The method of claim 34, wherein said step of detecting further includes detecting a proffered auditory emissions scan at a sensor configured to communicate with said system via at least one of a smartcard, reader, and network.

[c36] The method of claim 34, wherein said step of detecting a proffered auditory emissions scan includes detecting a proffered auditory emissions scan at least one of an infrared optical sensor, an auditory sensor, and a sound generator.

[c37] The method of claim 34, wherein said step of detecting includes at least one of: detecting, storing, and processing a proffered auditory emissions scan sample.

[c38] The method of claim 34, wherein said step of detecting further includes receiving a finite number of proffered auditory emissions scan samples during a transaction.

[c39] The method of claim 34, wherein said step of detecting further includes logging each proffered auditory emissions scan sample.

[c40] The method of claim 34, wherein said step of detecting further includes at least one of detecting, processing and storing at least one second proffered auditory emissions scan sample.

[c41] The method of claim 34, wherein said step of detecting further includes using said auditory emissions scan sensor to detect at least one of false noise associated with a device producing electronic auditory emissions.

[c42] The method of claim 34, wherein said step of verifying includes comparing a proffered auditory emissions scan sample with a stored auditory emissions scan sample.

[c43] The method of claim 42, wherein said step of comparing a proffered auditory emissions scan sample with a stored auditory emissions scan sample comprises storing, processing and comparing at least one auditory emissions scan characteristic including at least one of frequency, wavelength, and vibrations.

[c44] The method of claim 42, wherein comparing a proffered auditory emissions scan sample with a stored auditory emissions scan sample includes comparing a proffered auditory emissions scan sample with a biometric sample of at least one of a criminal, a terrorist, and a cardmember.

[c45] The method of claim 34, wherein said step of verifying includes verifying a proffered auditory emissions scan sample using information contained on at least one of a local database, a remote database, and a third-party controlled database.

[c46] The method of claim 34, wherein said step of verifying includes verifying a proffered auditory emissions scan sample using at least one of a local CPU and a third-party security vendor.